Checklist for Clean Workspace Security

Please follow these guidelines to secure your workstation or conference rooms and other common areas where you work.

☐ **Clean Desk Policy:** Many of the security requirements can be met by simply keeping an orderly workspace. Desks, credenzas, and workstations should be cleared and locked at the end of the day. The close tie between cleanliness and security is necessary.

Acceptable:	**Not Acceptable:**
• Trade journals and textbooks	• Any confidential documents
• Product documentation	• Phone lists with 7 digits or Rolodex
• General Training Material	• Organization Charts
• Internal phone only 4 digits	• Any electronic media (CDs, DVDs)
• Family photos, radio, phone	• Uncontained food
• Candy jar (sealed or wrapped candy)	• Any small electronic devices (PDA, cell, unsecured laptops, and other peripherals)
• Department Calendars	
• Monitor, keyboard, mouse, printer, or docking station	
• Large calculators with power cord	
• Laptops on secure cables	

☐ **Confidential or other sensitive information:** Clear workstations or meeting rooms of all work materials (including confidential items) at the end of the workday or when they will be unattended for extended periods during the business day. Confidential materials include client data, passwords, network information, product development specs, financials, direct-line phone lists, and other materials you would not want to fall into the wrong hands.

☐ **Access to your files, network and Lotus Notes:** You should always shut down your system before leaving. Turning off the monitor is not the same as shutting down the system. If you cannot shut down, use a password protected screen-saver. If you have Windows NT or Windows 200, use the lock-out feature.

☐ **Laptop computers:** All laptop computers should be secured in a locked cabinet or locked with a cable.

☐ **Palm Pilot or other small electronic devices:** These items should be secured in a locked cabinet or taken with you when leaving. This includes all hand-held computers, removable hard drives, and other computer peripherals, cameras, test equipment, video equipment, cell phone, and other valuables.

☐ **Security of drawers and cabinets:** Lock all drawers and cabinets, except pencil drawer. Use caution in leaving valuable in the pencil drawer.

☐ **Sensitive information in common areas:** Common areas should be secured. White boards, easel pads and computer screens displaying sensitive information should not be left unsecured or be visible through outside windows.

☐ **Proper disposal of sensitive media:** Be mindful of how you dispose of sensitive media and information. Back-up media, whether on tapes, CDs, or paper should not go in an open trash can. Sensitive media should be destroyed or locked up. *Confidential recycle bins can be used to dispose of any confidential information printed on paper. Contact your data disposal technician for details on how to dispose of large quantities of media.*

We appreciate your cooperation in helping the State of Utah Enterprise Information Security Office maintain a secure work environment for our employees, customers, and citizens.

Checklist for Clean Workspace Security

Please follow these guidelines to secure your workstation or conference rooms and other common areas where you work.

☐ **Clean Desk Policy:** Many of the security requirements can be met by simply keeping an orderly workspace. Desks, credenzas, and workstations should be cleared and locked at the end of the day. The close tie between cleanliness and security is necessary.

☐ **Confidential or other sensitive information:** Clear workstations or meeting rooms of all work materials (including confidential items) at the end of the workday or when they will be unattended for extended periods during the business day. Confidential materials include client data, passwords, network information, product development specs, financials, direct-line phone lists, and other materials you would not want to fall into the wrong hands.

☐ **Access to your files, network and Lotus Notes:** You should always shut down your system before leaving. Turning off the monitor is not the same as shutting down the system. If you cannot shut down, use a password protected screen-saver. If you have Windows NT or Windows 200, use the lock-out feature.

☐ **Laptop computers:** All laptop computers should be secured in a locked cabinet or locked with a cable.

☐ **Palm Pilot or other small electronic devices:** These items should be secured in a locked cabinet or taken with you when leaving. This includes all hand-held computers, removable hard drives, and other computer peripherals, cameras, test equipment, video equipment, cell phone, and other valuables.

☐ **Security of drawers and cabinets:** Lock all drawers and cabinets, except pencil drawer. Use caution in leaving valuable in the pencil drawer.

☐ **Sensitive information in common areas:** Common areas should be secured. White boards, easel pads and computer screens displaying sensitive information should not be left unsecured or be visible through outside windows.

☐ **Proper disposal of sensitive media:** Be mindful of how you dispose of sensitive media and information. Back-up media, whether on tapes, CDs, or paper should not go in an open trash can. Sensitive media should be destroyed or locked up. *Confidential recycle bins can be used to dispose of any confidential information printed on paper. Contact your data disposal technician for details on how to dispose of large quantities of media.*

We appreciate your cooperation in helping the State of Utah Enterprise Information Security Office maintain a secure work environment for our employees, customers and citizens.

Clean Workspace Security — Walkthrough Report

☐ All of your documents and equipment are safely secured.

Workspace Secured

We appreciate your cooperation in helping us maintain a secure environment for our employees, customers, and citizens.

Security Check date:

Clean Workspace Security — Walkthrough Report

Date:_____

Employee: _____

Manager:_____

Submitted by:_____

Security Violation

Please give you immediate attention to the following security vulnerabilities at you workspace.

☐ Workplace is not clean

☐ Confidential information not secured

☐ Laptop computer not secured

☐ Hand -held device not secure

☐ Small electronic equipment not secured

☐ Removable computer peripherals not secured

☐ PC left logged on to network

☐ PC left logged on to Lotus Notes

Additional Comments:

We appreciate your cooperation in helping the State of Utah EISO maintain a secure work environment for our employees, customers and citizens.